



50/P099/05 (A)

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 5月10日

出 願 番 号

Application Number:

特願2000-142307

出 願 人

Applicant(s):

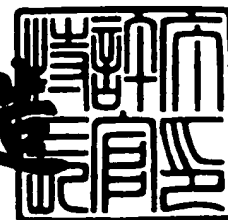
ソニー株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年 5月30日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3047344

【書類名】 特許願

【整理番号】 0000440503

【提出日】 平成12年 5月10日

【あて先】 特許庁長官殿

【国際特許分類】 H04K 1/00

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
内

【氏名】 大嶋 拓哉

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100094053

【弁理士】

【氏名又は名称】 佐藤 隆久

【手数料の表示】

【予納台帳番号】 014890

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707389

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信システム、通信装置および通信方法

【特許請求の範囲】

【請求項 1】

通信装置、サービス提供装置および管理装置を有し、前記サービス提供装置が提供するサービスあるいは商品に関する支払い処理を I C カードを用いて行う通信システムであって、

前記管理装置は、前記 I C カード内で支払い処理を行うための支払い処理情報を前記サービス提供装置からの支払い請求情報に基づいて生成し、当該支払い処理情報を当該管理装置と前記 I C カードとの間で共用される共通鍵を用いて暗号化し、当該暗号化した支払い処理情報と当該管理装置の署名情報とを前記通信装置に送信し、

前記通信装置は、前記管理装置から受信した前記署名情報の正当性を検証した後に、前記支払い処理情報を前記 I C カードに出力する通信システム。

【請求項 2】

前記管理装置は、当該管理装置の秘密鍵を用いて前記署名情報を作成し、

前記通信装置は、前記秘密鍵に対応する公開鍵を用いて前記署名情報の正当性を検証する

請求項 1 に記載の通信システム。

【請求項 3】

前記サービス提供装置は、支払い請求情報の正当性を示す署名情報を当該サービス提供装置の秘密鍵を用いて作成し、当該署名情報が付された前記支払い請求情報を、前記通信装置を介して前記管理装置に送信し、

前記管理装置は、前記サービス提供装置が作成した前記署名情報の正当性を前記サービス提供装置の秘密鍵に対応する公開鍵を用いて検証した後に、前記支払い処理情報と前記管理装置の前記署名情報とを前記通信装置に送信する

請求項 1 に記載の通信システム。

【請求項 4】

前記通信装置は、前記支払い請求情報の内容の表示あるいは音声出力を行い、当該内容に同意したことを示す指示をユーザから受けた後に、前記暗号化された前記支払い処理情報を前記 IC カードに出力する

請求項 1 に記載の通信システム。

【請求項 5】

前記管理装置は、前記共通鍵を用いて作成した前記 IC カードの残高情報読み出し要求を前記通信装置に送信し、前記 IC カードから読み出された残高情報を前記通信装置から受信し、当該残高情報を前記共通鍵を用いて復号し、

前記通信装置は、前記管理装置からの前記残高情報読み出し要求を前記 IC カードに送信し、前記 IC カードからの前記残高情報を前記管理装置に送信する

請求項 1 に記載の通信システム。

【請求項 6】

前記管理装置は、前記復号した残高情報を前記共通鍵で暗号化しないで前記支払い処理情報と共に前記通信装置に送信し、

前記通信装置は、前記管理装置から受信した前記残高情報が示す金額を表示あるいは音声出力し、当該金額に同意したことを示す指示をユーザから受けた後に、前記管理装置から受信した前記支払い処理情報を前記 IC カードに出力する

請求項 5 に記載の通信システム。

【請求項 7】

前記支払い処理情報は、前記 IC カード内で、当該 IC カードに記憶されている前記残高情報が示す金額から、前記支払い請求情報が示す金額を減算し、当該減算の結果を示す前記残高情報を前記 IC カードに記憶するための情報である

請求項 1 に記載の通信システム。

【請求項 8】

前記管理装置は、前記サービス提供装置が作成した前記支払い請求情報に基づいて、前記支払い処理に関しての所定の履歴情報を作成し、当該履歴情報を前記共通鍵で暗号化して前記支払い処理情報と共に前記通信装置に送信し、

前記通信装置は、前記管理装置から受信した前記履歴情報を前記 IC カードに

出力する

請求項 1 に記載の通信システム。

【請求項 9】

前記通信装置は、前記支払い処理情報に応じた支払い処理が適切に行われたことを示す通知を前記 IC カードから入力すると、当該通知を前記管理装置に送信する

請求項 1 に記載の通信システム。

【請求項 1 0】

前記管理装置は、前記通信装置から前記通知を受信すると、支払いが完了したことを示す支払い完了通知を前記通信装置および前記サービス提供装置に送信する

請求項 9 に記載の通信システム。

【請求項 1 1】

前記通信装置は、前記 IC カードにアクセス可能なアクセス装置との間で、前記支払い処理情報の出力、並びに所定の情報の入出力を行う

請求項 1 に記載の通信システム。

【請求項 1 2】

前記通信装置は、ブラウザプログラムを実行して前記サービス提供装置との間で通信を行い、当該ブラウザプログラムを実行中に、所定のインターフェースプログラムを実行して前記アクセス装置を介して前記 IC カードとの間で情報の入出力を行う

請求項 1 1 に記載の通信システム。

【請求項 1 3】

前記サービス提供装置は、前記支払い請求情報と共に前記インターフェースプログラムを前記通信装置に送信する

請求項 1 1 に記載の通信システム。

【請求項 1 4】

前記通信装置は、前記サービス提供装置との間で、当該サービス提供装置が提供するサービスあるいは商品を受けるための所定の情報の送受信を行う

請求項 1 に記載の通信システム。

【請求項 1 5】

前記サービス提供装置は、

前記サービスあるいは商品に関しての支払い手続を行う旨の指示を前記通信装置から受けると、当該サービスあるいは商品についての前記支払い請求情報を前記通信装置に送信し、

前記通信装置は、前記サービス提供装置から受信した支払い請求情報の内容を表示あるいは出力し、当該内容に同意したことを示す指示をユーザから受けた後に、前記支払い請求情報を前記管理装置に送信する

請求項 1 4 に記載の通信システム。

【請求項 1 6】

前記管理装置は、

前記共通鍵を保持し、前記支払い処理情報の生成、並びに前記共通鍵を用いた暗号化を行う第 1 の管理装置と、

前記第 1 の管理装置から入力した前記暗号化された前記支払い処理情報について当該管理装置の秘密鍵を用いて前記署名情報を作成し、前記暗号化された支払い処理情報と前記署名情報とを前記通信装置に送信する第 2 の管理装置と

を有する

請求項 1 に記載の通信システム。

【請求項 1 7】

前記通信装置および前記管理装置は、

前記通信装置と前記管理装置との間で情報または要求を送受信する際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において当該秘密鍵に対応する公開鍵を用いて検証する

請求項 1 に記載の通信システム。

【請求項 1 8】

前記通信装置および前記サービス提供装置は、

前記通信装置と前記サービス提供装置との間で情報または要求を送受信する際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において当該秘密鍵に

対応する公開鍵を用いて検証する

請求項 1 に記載の通信システム。

【請求項 1 9】

前記通信装置、前記サービス提供装置および前記管理装置は、ネットワークを介して前記情報の送受信を行う

請求項 1 に記載の通信システム。

【請求項 2 0】

サービス提供装置が提供するサービスあるいは商品に対しての支払い処理を IC カードを用いて行う場合に、当該 IC カードとの間で情報の入出力を行う他の通信装置との間で通信を行う通信装置であって、

前記 IC カード内で支払い処理を行うための支払い処理情報を当該通信装置と前記 IC カードとの間で共用される共通鍵を用いて暗号化し、当該暗号化した支払い処理情報の正当性を示す当該通信装置の署名情報を生成し、前記暗号化した支払い処理情報と前記署名情報とを前記他の通信装置に送信する

通信装置。

【請求項 2 1】

当該通信装置の秘密鍵を用いて前記署名情報を作成する

請求項 2 0 に記載の通信装置。

【請求項 2 2】

前記サービス提供装置が作成した署名情報の正当性を、前記サービス提供装置の秘密鍵に対応する公開鍵を用いて検証した後に、前記支払い処理情報と前記管理装置の前記署名情報とを前記他の通信装置に送信する

請求項 2 0 に記載の通信装置。

【請求項 2 3】

前記共通鍵を保持し、前記支払い処理情報の生成、並びに前記共通鍵を用いた前記支払い処理情報の暗号化を行う第 1 の管理装置と、

前記第 1 の管理装置から入力した前記暗号化された前記支払い処理情報について当該通信装置の秘密鍵を用いて前記署名情報を作成し、前記暗号化された支払い処理情報と前記署名情報とを前記他の通信装置に送信する第 2 の管理装置と

を有する

請求項 2 0 に記載の通信装置。

【請求項 2 4】

通信装置、サービス提供装置および管理装置を用いて、前記サービス提供装置が提供したあるいは提供するサービスあるいは商品に対しての支払い処理を I C カードを用いて行う通信方法であって、

前記管理装置において、前記 I C カード内で支払い処理を行うための支払い処理情報を前記サービス提供装置からの支払い請求情報に基づいて生成し、当該支払い処理情報を当該管理装置と前記 I C カードとの間で共用される共通鍵を用いて暗号化し、

当該暗号化した支払い処理情報と当該管理装置の署名情報とを前記管理装置から前記通信装置に送信し、

前記通信装置において、前記管理装置から受信した前記署名情報の正当性を検証した後に、前記支払い処理情報を前記 I C カードに出力する

通信方法。

【請求項 2 5】

前記管理装置において、当該管理装置の秘密鍵を用いて前記署名情報を作成し

前記通信装置において、前記秘密鍵に対応する公開鍵を用いて前記署名情報の正当性を検証する

請求項 2 4 に記載の通信方法。

【請求項 2 6】

前記サービス提供装置において、支払い請求情報の正当性を示す署名情報を当該サービス提供装置の秘密鍵を用いて作成し、

当該署名情報が付された前記支払い請求情報を、前記通信装置を介して前記サービス提供装置から前記管理装置に送信し、

前記管理装置において、前記サービス提供装置が作成した前記署名情報の正当性を前記サービス提供装置の秘密鍵に対応する公開鍵を用いて検証した後に、前記支払い処理情報と前記管理装置の前記署名情報とを前記通信装置に送信する



請求項 2 4 に記載の通信方法。

【請求項 2 7】

前記通信装置において、前記支払い請求情報の内容の表示あるいは音声出力を行い、当該内容に同意したことを示す指示をユーザから受けた後に、前記暗号化された前記支払い処理情報を前記 I C カードに出力する

請求項 2 4 に記載の通信方法。

【請求項 2 8】

前記共通鍵を用いて作成した前記 I C カードの残高情報読み出し要求を前記管理装置から前記通信装置に送信し、

前記通信装置において、前記管理装置からの前記残高情報読み出し要求を前記 I C カードに出力し、

前記 I C カードにおいて、前記通信装置から入力した前記残高情報読み出し要求に応じて、当該 I C カード内の記憶回路から残高情報を読み出し、当該読み出した残高情報を通信装置を介して前記管理装置に送信し、

前記管理装置において、前記通信装置から受信した残高情報を前記共通鍵を用いて復号する

請求項 2 4 に記載の通信方法。

【請求項 2 9】

前記管理装置から前記通信装置に、前記復号した残高情報を前記共通鍵で暗号化しないで前記支払い処理情報と共に送信し、

前記通信装置において、前記管理装置から受信した前記残高情報が示す金額を表示あるいは音声出力し、当該金額に同意したことを示す指示をユーザから受けた後に、前記管理装置から受信した前記支払い処理情報を前記 I C カードに出力する

請求項 2 4 に記載の通信方法。

【請求項 3 0】

前記支払い処理情報は、前記 I C カード内で、当該 I C カードに記憶されている前記残高情報が示す金額から、前記支払い請求情報が示す金額を減算し、当該減算の結果を示す前記残高情報を記憶するための情報である

請求項 2 4 に記載の通信方法。

【請求項 3 1】

前記管理装置において、前記サービス提供装置が作成した前記支払い請求情報に基づいて、前記支払い処理に関しての所定の履歴情報を作成し、当該履歴情報を前記共通鍵で暗号化し、

当該暗号化した前記履歴情報を前記支払い処理情報と共に前記管理装置から前記通信装置に送信し、

前記通信装置において、前記管理装置から受信した前記残高情報が示す金額に同意したことを示す指示をユーザから受けた後に、前記管理装置から受信した前記履歴情報を前記 IC カードに出力し、

前記 IC カードは、前記通信装置から入力した前記履歴情報を記憶する

請求項 2 4 に記載の通信方法。

【請求項 3 2】

前記通信装置は、前記 IC カードにアクセス可能なアクセス装置との間で、前記支払い処理情報の出力、並びに所定の情報の入出力を行う

請求項 2 4 に記載の通信方法。

【請求項 3 3】

前記 IC カードは、耐タンパ性のモジュール内で、前記支払い処理情報に応じた前記支払い処理を行う

請求項 2 4 に記載の通信方法。

【請求項 3 4】

前記通信装置と前記管理装置との間で情報または要求を送受信する際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において当該秘密鍵に対応する公開鍵を用いて検証する

請求項 2 4 に記載の通信方法。

【請求項 3 5】

前記通信装置および前記サービス提供装置は、

前記通信装置と前記サービス提供装置との間で情報または要求を送受信する際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において当該秘密鍵に

対応する公開鍵を用いて検証する

請求項 2 4 に記載の通信方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、共通鍵を保持した I C カードを用いて、ネットワークなどを用いた決済処理を安全に行うことができる通信システム、通信装置および通信方法に関する。

【 0 0 0 2 】

【従来の技術】

ネットワークを介した電子商取引を安全に行うために、通常、P K I (Public Key Infrastructure: 公開鍵インフラ) プロトコルが採用されている。

P K I プロトコルでは、送信元で秘密鍵を用いて署名情報を作成し、送信先から送信先に、当該署名情報を伝送情報と共に送信する。そして、送信先において、当該秘密鍵に対応する公開鍵を用いて当該署名情報の検証を行うことで、受信した伝送情報が正当な送信元で作成されたものであるか否かを判断する。

【 0 0 0 3 】

ところで、近年、I C (Integrated Circuit) カードを用いて、ネットワークを介した電子商取引を行う試みがある。

ここで、通常、I C カードは、共通鍵を保持しており、共通鍵暗号方式を用いて秘匿性のある情報の入出力を行う。このような I C カードは、共通鍵が署名情報を作成するための鍵とはなり得ないため、I C カードを紛失した場合でも、被害を小さくできるという利点がある。

【 0 0 0 4 】

【発明の解決しようとする課題】

しかしながら、ネットワークを介した電子商取引を安全に行うためには、秘密鍵を用いて署名情報を作成する必要があるが、従来の手法では、I C カードが秘密鍵を保持（記憶）していないため、署名情報の作成ができないという問題がある。

この場合に、ＩＣカードに秘密鍵を保持する方法も考えられるが、前述したように、秘密鍵は署名情報を作成できるため印鑑照明と同様の効力があり、ＩＣカードを紛失して悪用されたときの被害が大きすぎるという問題がある。

また、上述したようなＩＣカードが採用する共通鍵暗号方式のみを用いて、ネットワークを介した電子商取引を行うと、取り引きを行う多数の相手先のサーバ装置などが共通鍵を持つことになり、共通鍵が盗まれたり、悪用される可能性が高くなるという問題もある。

#### 【 0 0 0 5 】

本発明は上述した従来技術の問題点に鑑みてなされ、共通鍵を保持したＩＣカードを用いて、ネットワークを介した電子商取引を安全に行うことができる通信システム、通信装置および通信方法を提供することを目的とする。

#### 【 0 0 0 6 】

##### 【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、第１の発明の通信システムは、通信装置、サービス提供装置および管理装置を有し、前記サービス提供装置が提供するサービスあるいは商品に関する支払い処理をＩＣカードを用いて行う通信システムであって、前記管理装置は、前記ＩＣカード内で支払い処理を行うための支払い処理情報を前記サービス提供装置からの支払い請求情報に基づいて生成し、当該支払い処理情報を当該管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化し、当該暗号化した支払い処理情報と当該管理装置の署名情報とを前記通信装置に送信し、前記通信装置は、前記管理装置から受信した前記署名情報の正当性を検証した後に、前記支払い処理情報を前記ＩＣカードに出力する。

#### 【 0 0 0 7 】

第１の発明の通信システムの作用は以下ようになる。

サービス提供装置において、サービスあるいは商品を提供したことに関する情報が生成され、当該情報が管理装置に送信される。

次に、管理装置は、前記ＩＣカード内で支払い処理を行うための支払い処理情報を前記サービス提供装置からの支払い請求情報に基づいて生成し、当該支払い

処理情報を当該管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化し、当該暗号化した支払い処理情報と当該管理装置の署名情報とを前記通信装置に送信する。

次に、前記通信装置は、前記管理装置から受信した前記署名情報の正当性を検証した後に、前記支払い処理情報を前記ＩＣカードに出力する。

第１の発明の通信システムでは、支払い処理情報は、前記管理装置と前記ＩＣカードとの間で共用される共通鍵を用いて暗号化されているため、安全性が保たれる。すなわち、当該共通鍵は、前記管理装置と前記ＩＣカードとの間でのみ共用され、それ以外の装置には供給されないため、共通鍵の管理が容易であると共に、共通鍵を不正に取得される可能性を低くできる。また、共通鍵をＩＣカード内の耐タンパ性のメモリに記憶し、ＩＣカードの外部に読み出しできないようにすることで、ＩＣカードのユーザであっても、当該共通鍵を用いて支払い処理情報を不正に改竄できない。

また、第１の発明の通信システムでは、支払い処理情報に管理装置の署名情報を付して通信装置に送信し、通信装置において、受信した署名情報を検証することで、支払い処理情報が通信経路上で不正に改竄されたか否かを通信装置で検証でき、通信経路上での安全性を保証できる。

#### 【 0 0 0 8 】

また、第１の発明の通信システムは、好ましくは、前記管理装置は、当該管理装置の秘密鍵を用いて前記署名情報を作成し、前記通信装置は、前記秘密鍵に対応する公開鍵を用いて前記署名情報の正当性を検証する。

#### 【 0 0 0 9 】

また、第１の発明の通信システムは、好ましくは、前記サービス提供装置は、前記支払い請求情報の正当性を示す署名情報を当該サービス提供装置の秘密鍵を用いて作成し、当該署名情報が付された前記支払い請求情報を、前記通信装置を介して前記管理装置に送信し、前記管理装置は、前記サービス提供装置が作成した前記署名情報の正当性を、前記サービス提供装置の秘密鍵に対応する公開鍵を用いて検証した後に、前記支払い処理情報と前記管理装置の前記署名情報とを前記通信装置に送信する。

## 【 0 0 1 0 】

また、第 1 の発明の通信システムは、好ましくは、前記通信装置は、前記支払い請求情報の内容の表示あるいは音声出力を行い、当該内容に同意したことを示す指示をユーザから受けた後に、前記暗号化された前記支払い処理情報を前記 IC カードに出力する。

## 【 0 0 1 1 】

また、第 1 の発明の通信システムは、好ましくは、前記管理装置は、前記共通鍵を用いて作成した前記 IC カードの残高情報読み出し要求を前記通信装置に送信し、前記 IC カードから読み出された残高情報を前記通信装置から受信し、当該残高情報を前記共通鍵を用いて復号し、前記通信装置は、前記管理装置からの前記残高情報読み出し要求を前記 IC カードに送信し、前記 IC カードからの前記残高情報を前記管理装置に送信する。

## 【 0 0 1 2 】

また、第 1 の発明の通信システムは、好ましくは、前記管理装置は、前記復号した残高情報を前記共通鍵で暗号化しないで前記支払い処理情報と共に前記通信装置に送信し、前記通信装置は、前記管理装置から受信した前記残高情報が示す金額を表示あるいは音声出力し、当該金額に同意したことを示す指示をユーザから受けた後に、前記管理装置から受信した前記支払い処理情報を前記 IC カードに出力する。

## 【 0 0 1 3 】

また、第 1 の発明の通信システムは、好ましくは、前記支払い処理情報は、前記 IC カード内で、当該 IC カードに記憶されている前記残高情報が示す金額から、前記支払い請求情報が示す金額を減算し、当該減算の結果を示す前記残高情報を記憶するための情報である。

## 【 0 0 1 4 】

また、第 1 の発明の通信システムは、好ましくは、前記管理装置は、前記サービス提供装置が作成した前記支払い請求情報に基づいて、前記支払い処理に関しての所定の履歴情報を作成し、当該履歴情報を前記共通鍵で暗号化して前記支払い処理情報と共に前記通信装置に送信し、前記通信装置は、前記管理装置から受

信した前記履歴情報を前記 I C カードに出力する。

【 0 0 1 5 】

また、第 1 の発明の通信システムは、好ましくは、前記通信装置は、前記支払い処理情報に応じた支払い処理が適切に行われたことを示す通知を前記 I C カードから入力すると、当該通知を前記管理装置に送信する。

【 0 0 1 6 】

また、第 1 の発明の通信システムは、好ましくは、前記管理装置は、前記通信装置から前記通知を受信すると、支払いが完了したことを示す支払い完了通知を前記通信装置および前記サービス提供装置に送信する。

【 0 0 1 7 】

また、第 1 の発明の通信システムは、好ましくは、前記通信装置は、前記 I C カードにアクセス可能なアクセス装置との間で、前記支払い処理情報の出力、並びに所定の情報の入出力を行う。

【 0 0 1 8 】

また、第 1 の発明の通信システムは、好ましくは、前記通信装置は、ブラウザプログラムを実行して前記サービス提供装置との間で通信を行い、当該ブラウザプログラムを実行中に、所定のインターフェースプログラムを実行して前記アクセス装置を介して前記 I C カードとの間で情報の入出力を行う。

【 0 0 1 9 】

また、第 1 の発明の通信システムは、好ましくは、前記サービス提供装置は、前記支払い請求情報と共に前記インターフェースプログラムを前記通信装置に送信する。

【 0 0 2 0 】

また、第 1 の発明の通信システムは、好ましくは、前記通信装置は、前記サービス提供装置との間で、当該サービス提供装置が提供するサービスあるいは商品を受けるための所定の情報の送受信を行う。

【 0 0 2 1 】

また、第 1 の発明の通信システムは、好ましくは、前記サービス提供装置は、前記サービスあるいは商品に関しての支払い手続を行う旨の指示を前記通信装置

から受けると、当該サービスあるいは商品についての前記支払い請求情報を前記通信装置に送信し、前記通信装置は、前記サービス提供装置から受信した支払い請求情報の内容を表示あるいは出力し、当該内容に同意したことを示す指示をユーザから受けた後に、前記支払い請求情報を前記管理装置に送信する。

【 0 0 2 2 】

また、第 1 の発明の通信システムは、好ましくは、前記管理装置は、前記共通鍵を保持し、前記支払い処理情報の生成、並びに前記共通鍵を用いた暗号化を行う第 1 の管理装置と、前記第 1 の管理装置から入力した前記暗号化された前記支払い処理情報について当該管理装置の秘密鍵を用いて前記署名情報を作成し、前記暗号化された支払い処理情報と前記署名情報とを前記通信装置に送信する第 2 の管理装置とを有する。

【 0 0 2 3 】

また、第 1 の発明の通信システムは、好ましくは、前記通信装置および前記管理装置は、前記通信装置と前記管理装置との間で情報または要求を送受信する際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において当該秘密鍵に対応する公開鍵を用いて検証する。

【 0 0 2 4 】

また、第 1 の発明の通信システムは、好ましくは、前記通信装置および前記サービス提供装置は、前記通信装置と前記サービス提供装置との間で情報または要求を送受信する際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において当該秘密鍵に対応する公開鍵を用いて検証する。

【 0 0 2 5 】

また、第 1 の発明の通信システムは、好ましくは、前記通信装置、前記サービス提供装置および前記管理装置は、ネットワークを介して前記情報の送受信を行う。

【 0 0 2 6 】

また、第 2 の発明の通信装置は、サービス提供装置が提供するサービスあるいは商品に対しての支払い処理を IC カードを用いて行う場合に、当該 IC カードとの間で情報の入出力を行う他の通信装置および管理装置との間で通信を行う通



信装置であって、前記 I C カード内で支払い処理を行うための支払い処理情報を当該通信装置と前記 I C カードとの間で共用される共通鍵を用いて暗号化し、当該暗号化した支払い処理情報の正当性を示す当該通信装置の署名情報を生成し、前記暗号化した支払い処理情報と前記署名情報とを前記他の通信装置に送信する。

【 0 0 2 7 】

第 2 の発明の通信装置の作用は以下になる。

まず、前記 I C カード内で支払い処理を行うための支払い処理情報を当該通信装置と前記 I C カードとの間で共用される共通鍵を用いて暗号化する。

次に、当該暗号化した支払い処理情報の正当性を示す当該通信装置の署名情報を生成する。

次に、前記暗号化した支払い処理情報と前記署名情報とを前記他の通信装置に送信する。

【 0 0 2 8 】

また、第 2 の発明の通信装置は、好ましくは、当該通信装置の秘密鍵を用いて前記署名情報を作成する。

【 0 0 2 9 】

また、第 2 の発明の通信装置は、好ましくは、前記サービス提供装置が作成した前記署名情報の正当性を、前記サービス提供装置の秘密鍵に対応する公開鍵を用いて検証した後に、前記支払い処理情報と前記管理装置の前記署名情報とを前記他の通信装置に送信する。

【 0 0 3 0 】

また、第 2 の発明の通信装置は、好ましくは、前記共通鍵を保持し、前記支払い処理情報の生成、並びに前記共通鍵を用いた暗号化を行う第 1 の管理装置と、前記第 1 の管理装置から入力した前記暗号化された前記支払い処理情報について当該通信装置の秘密鍵を用いて前記署名情報を作成し、前記暗号化された支払い処理情報と前記署名情報とを前記他の通信装置に送信する第 2 の管理装置とを有する。

## 【 0 0 3 1 】

また、第 3 の発明の通信方法は、前記管理装置において、前記 I C カード内で支払い処理を行うための支払い処理情報を前記サービス提供装置からの情報に基づいて生成し、当該支払い処理情報を当該管理装置と前記 I C カードとの間で共用される共通鍵を用いて暗号化し、当該暗号化した支払い処理情報と当該管理装置の署名情報とを前記管理装置から前記通信装置に送信し、前記通信装置において、前記管理装置から受信した前記署名情報の正当性を検証した後に、前記支払い処理情報を前記 I C カードに出力する。

## 【 0 0 3 2 】

また、第 3 の発明の通信方法は、前記管理装置において、当該管理装置の秘密鍵を用いて前記署名情報を作成し、前記通信装置において、前記秘密鍵に対応する公開鍵を用いて前記署名情報の正当性を検証する。

## 【 0 0 3 3 】

また、第 3 の発明の通信方法は、前記サービス提供装置において、前記支払い請求情報の正当性を示す署名情報を当該サービス提供装置の秘密鍵を用いて作成し、当該署名情報が付された前記支払い請求情報を、前記通信装置を介して前記サービス提供装置から前記管理装置に送信し、前記管理装置において、前記サービス提供装置が作成した前記署名情報の正当性を、前記サービス提供装置の秘密鍵に対応する公開鍵を用いて検証した後に、前記支払い処理情報と前記管理装置の前記署名情報とを前記通信装置に送信する。

## 【 0 0 3 4 】

また、第 3 の発明の通信方法は、好ましくは、前記通信装置は、前記 I C カードにアクセス可能なアクセス装置との間で、前記支払い処理情報の出力、並びに所定の情報の入出力を行う。

## 【 0 0 3 5 】

また、第 3 の発明の通信方法は、好ましくは、前記 I C カードは、耐タンパ性のモジュール内で、前記支払い処理情報に応じた前記支払い処理を行う

【 0 0 3 6 】

【発明の実施の形態】

以下、本発明の実施形態に係わるネットワークシステムについて説明する。

図 1 は、本実施形態のネットワークシステム 1 の全体構成図である。

図 1 に示すように、ネットワークシステム 1 は、ユーザ 2、決済機関 3 および店舗 4 の間でネットワーク 5 を介した通信を行う。

〔ユーザ 2〕

ユーザ 2 には、IC カード 2 0 にアクセスを行うための R/W 装置 2 1 およびパーソナルコンピュータ 2 2 が設けられている。

ここで、IC カード 2 0 が第 1 ～ 3 の発明の IC カードに対応し、パーソナルコンピュータ 2 2 が第 1 および第 3 の発明の通信装置、第 2 の発明の他の通信装置に対応している。また、IC カード R/W 装置 2 1 が本発明のアクセス装置に対応している。

【 0 0 3 7 】

IC カード 2 0 は、図 2 (A) に示すように耐タンパ性の IC モジュール 5 0 を有し、図 2 (B) に示すように当該 IC モジュール 5 0 内に処理回路 5 1 およびメモリ 5 2 を内蔵している。

処理回路 5 1 は、共通鍵を用いた復号処理、所定の情報および要求に応じた処理、並びに相互認証処理などの種々の処理を行う。

メモリ 5 2 は、決済機関 3 のセキュリティサーバ 3 1 との間で共用する共通鍵  $K_C$  を記憶している。

IC カード 2 0 は、図 3 に示すように、IC カード R/W 装置 2 1、インターフェースプログラム 2 4、ブラウザプログラム 2 3、パーソナルコンピュータ 2 2、ネットワーク 5 およびアプリケーションサーバ 3 0 を介して、セキュリティサーバ 3 1 との間で送受信する情報を、共通鍵  $K_C$  を用いた共通鍵暗号方式によって暗号化および復号する。

【 0 0 3 8 】

IC カード R/W 装置 2 1 は、IC カード 2 0 の IC モジュール 5 0 との間で非接触方式あるいは接触方式でデータ入出力を行うと共に、パーソナルコンピュ

ータ 2 2 との間との間で情報および要求の入出力を行う。

【 0 0 3 9 】

パーソナルコンピュータ 2 2 は、ユーザによるキーボードやマウスなどの操作に応じて、ブラウザプログラム 2 3 を実行すると共に、ブラウザプログラム 2 3 上で、後述するようにネットワーク 5 を介して決済機関 3 のアプリケーションサーバ 3 0 から受信したインターフェースプログラム 2 4 を実行する。

パーソナルコンピュータ 2 2 は、ディスプレイ、キーボードおよびマウスなどを有している。

ここで、インターフェースプログラム 2 4 が第 1 および第 3 の発明のインターフェースプログラムに対応している。

【 0 0 4 0 】

ブラウザプログラム 2 3 は、図 4 に示すように、パーソナルコンピュータ 2 2 上で動作するプログラムであり、店舗 4 のネットワークサーバ 4 0 の HTTPS レイヤ 6 0 との間で、PKI プロトコルにより、送信元において自らの秘密鍵を用いた署名情報の付加、並びに送信先において当該秘密鍵に対応する公開鍵を用いた当該署名情報の検証を行う。

【 0 0 4 1 】

インターフェースプログラム 2 4 は、図 5 に示すように、パーソナルコンピュータ 2 2 上で動作し、決済機関 3 のアプリケーションサーバ 3 0 の APS 上位レイヤ 3 0 a との間で、PKI プロトコルにより、送信元において自らの秘密鍵を用いた署名情報の付加、並びに送信先において当該秘密鍵に対応する公開鍵を用いた当該署名情報の検証を行う。

また、インターフェースプログラム 2 4 は、ブラウザプログラム 2 3 を実行中に、R/W 装置 2 1 を介して IC カード 2 0 などのローカル資源へのアクセスを容易に実現するための機能拡張プログラムである。

【 0 0 4 2 】

〔決済機関 3〕

決済機関 3 には、アプリケーションサーバ 3 0、セキュリティサーバ 3 1 および情報管理サーバ 3 2 が設けられている。

ここで、アプリケーションサーバ 3 0、セキュリティサーバ 3 1 および情報管理サーバ 3 2 が、第 1 および第 3 の発明の管理装置および第 2 の発明の通信装置に対応している。

また、セキュリティサーバ 3 1 が本発明の第 1 の管理装置に対応し、アプリケーションサーバ 3 0 が本発明の第 2 の管理装置に対応している。

アプリケーションサーバ 3 0 は、ネットワーク 5 を介して、パーソナルコンピュータ 2 2 およびネットワークサーバ 4 0 と通信が可能である。

また、アプリケーションサーバ 3 0 は、店舗 4 のネットワークサーバ 4 0 の秘密鍵  $K_{SHOP,S}$  に対応した公開鍵  $K_{SHOP,P}$  を保持し、後述するように、ネットワークサーバ 4 0 が生成した金額情報  $BILL$  に付された署名情報  $SIG$  を検証する。

また、アプリケーションサーバ 3 0 は、図 5 に示すように、APS 上位レイヤ 3 0 a および APS 下位レイヤ 3 0 b を有する。

#### 【0043】

セキュリティサーバ 3 1 は、ユーザ 2 の IC カード 2 0 との間で共用する共通鍵  $K_C$  を記憶している。

セキュリティサーバ 3 1 は、図 3 に示すように、IC カード R/W 装置 2 1、インターフェースプログラム 2 4、ブラウザプログラム 2 3、パーソナルコンピュータ 2 2、ネットワーク 5 およびアプリケーションサーバ 3 0 を介して、IC カード 2 0 との間で送受信する情報を、共通鍵  $K_C$  を用いた共通鍵暗号方式によって暗号化および復号する。

#### 【0044】

情報管理サーバ 3 2 は、例えば、登録されたユーザの個人情報を記憶および管理する。

#### 【0045】

##### 〔店舗 4〕

店舗 4 には、ネットワークサーバ 4 0 が設けられている。

ここで、ネットワークサーバ 4 0 が本発明のサービス提供装置に対応している。

ネットワークサーバ 4 0 は、図 4 に示すように、パーソナルコンピュータ 2 2 上で動作するブラウザプログラム 2 3 との間で、パーソナルコンピュータ 2 2 上で動作するプログラムである。

また、ネットワークサーバ 4 0 は、例えば、商品あるいはサービスの紹介情報を記憶すると共に、店舗 4 がユーザ 2 に請求する金額を示す請求額情報 B I L L (本発明の支払い請求情報) と、当該請求額情報に対して自らの秘密鍵  $K_{SHOP,S}$  を用いて作成した署名情報 S I G とを生成する。

【 0 0 4 6 】

以下、図 1 に示すネットワークシステム 1 の動作を説明する。

図 6 は、ネットワークシステム 1 の動作を説明するための図である。

先ず、図 6 に示すユーザによる商品決定が行われる前に、ユーザ 2 がパーソナルコンピュータ 2 2 上で動作するブラウザプログラム 2 3 を用いて、ネットワーク 5 を介して、店舗 4 のネットワークサーバ 4 0 にアクセスを行う。当該アクセスにより、ネットワーク 5 を介してネットワークサーバ 4 0 からパーソナルコンピュータ 2 2 に、店舗 4 が提供する商品情報が送信され、それに応じた画面がパーソナルコンピュータ 2 2 のディスプレイに表示される。

【 0 0 4 7 】

以下、ネットワークシステム 1 の動作を図 6 ～図 8 に示す各ステップ毎に説明する。

なお、以下に示す動作において、パーソナルコンピュータ 2 2 とネットワークサーバ 4 0 との間で情報あるいは要求の送受信を行う際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において、当該秘密鍵に対応する公開鍵を用いて検証するが、当該処理については記載を省略する。

また、同様に、パーソナルコンピュータ 2 2 とアプリケーションサーバ 3 0 との間で情報あるいは要求の送受信を行う際に、送信元の秘密鍵を用いて作成した署名情報を、送信先において、当該秘密鍵に対応する公開鍵を用いて検証するが、当該処理についてはステップ S T 1 4 , S T 1 5 を除いて記載を省略する。

【 0 0 4 8 】

ステップ S T 1 :

パーソナルコンピュータ 2 2 とネットワークサーバ 4 0 との間で S S L (Secure Socket Layer) を用いた相互認証を行い、セキュアな通信路を確立する。

ステップ S T 2 :

ユーザ 2 が、パーソナルコンピュータ 2 2 のキーボードやマウスなどを操作して購入を希望する商品を決定すると、それに応じた商品決定情報がパーソナルコンピュータ 2 2 からネットワークサーバ 4 0 に送信される。

ステップ S T 3 :

ネットワークサーバ 4 0 は、パーソナルコンピュータ 2 2 から商品決定情報を受けると、その見積もり情報をパーソナルコンピュータ 2 2 に送信する。

ステップ S T 4 :

パーソナルコンピュータ 2 2 は、ネットワークサーバ 4 0 から受けた見積もり情報をディスプレイに表示する。ユーザ 2 は、当該見積もりに同意した場合には、パーソナルコンピュータ 2 2 のキーボードなどを操作して請求額要求をネットワークサーバ 4 0 に出す。

【 0 0 4 9 】

ステップ S T 5 :

ネットワークサーバ 4 0 は、パーソナルコンピュータ 2 2 から請求額要求を受けると、店舗 4 がユーザ 2 に請求する金額を示す請求額情報 B I L L と、当該請求額情報 B I L L に対して自らの秘密鍵  $K_{SHOP,S}$  を用いて作成した署名情報 S I G と、インターフェースプログラム 2 4 とをパーソナルコンピュータ 2 2 に送信する。

ステップ S T 6 :

パーソナルコンピュータ 2 2 は、ステップ S T 5 でネットワークサーバ 4 0 から受信した請求額情報 B I L L が示す金額をディスプレイに表示する。

【 0 0 5 0 】

ステップ S T 7 :

ステップ S T 6 でディスプレイに表示された金額に同意したユーザ 2 がパーソナルコンピュータ 2 2 のキーボードなどを用いて所定の指示を出すと、ステップ S T 5 でネットワークサーバ 4 0 から受信したインターフェースプログラム 2 4

が起動される。

そして、パーソナルコンピュータ22は、起動されたインターフェースプログラム24を用いて、決済機関3のアプリケーションサーバ30との間でSSLを用いた相互認証を行い、セキュアな通信路を確立する。

#### 【0051】

##### ステップST8：

パーソナルコンピュータ22は、ステップST5で店舗4のネットワークサーバ40から受信した請求額情報BILLと、当該請求額情報に対しての署名情報SIGとを含む決済要求を決済機関3のアプリケーションサーバ30に送信する。

##### ステップST9：

アプリケーションサーバ30は、例えば、情報管理サーバ32から読み出した店舗4に対応する公開鍵 $K_{SHOP,P}$ を用いて、ステップST8で受信した署名情報SIGを検証し、当該署名情報SIGが店舗4のネットワークサーバ40において付された正当なものであると判断すると、ステップST10の処理を行う。

なお、アプリケーションサーバ30は、署名情報SIGが不正なものであると判断した場合には、例えば、パーソナルコンピュータ22に対してのその旨を通知した後、処理を終了する。

#### 【0052】

##### ステップST10：

アプリケーションサーバ30は、例えば、請求額情報BILLを含む決済要求をセキュリティサーバ31に送信する。

##### ステップST11：

セキュリティサーバ31は、ICカード20から決済要求を受けると、ICカード20との間で相互認証を行い、ICカード20との間で用いる共通鍵 $K_C$ からセッション鍵 $K_{SES}$ を生成する。

また、ICカード20でも、同様に、共通鍵 $K_C$ からセッション鍵 $K_{SES}$ を生成する。



【 0 0 5 3 】

ステップ S T 1 2 :

セキュリティサーバ 3 1 は、残高読み出し要求 B R C (本発明の残高情報読み出し要求) を生成し、これをセッション鍵  $K_{SES}$  で暗号化してアプリケーションサーバ 3 0 に出力する。

アプリケーションサーバ 3 0 は、セキュリティサーバ 3 1 から入力した残高読み出し要求 B R C を、パーソナルコンピュータ 2 2 に送信する。

パーソナルコンピュータ 2 2 は、アプリケーションサーバ 3 0 から受信した残高読み出し要求 B R C を、I C カード R / W 装置 2 1 を介して I C カード 2 0 に出力する。

【 0 0 5 4 】

ステップ S T 1 3 :

I C カード 2 0 は、パーソナルコンピュータ 2 2 からの残高読み出し要求 B R C を入力すると、これをステップ S T 1 1 で生成したセッション鍵  $K_{SES}$  を用いて復号する。

そして、I C カード 2 0 は、残高読み出し要求 B R C に応じた処理回路 5 1 の処理によって、I C カード 2 0 内の耐タンパ性のメモリ 5 2 から残高情報 B I (本発明の残高情報) を読み出し、これをセッション鍵  $K_{SES}$  を用いて暗号化した後に、パーソナルコンピュータ 2 2 に出力する。

パーソナルコンピュータ 2 2 は、I C カード 2 0 からの残高情報 B I を、アプリケーションサーバ 3 0 に送信する。

アプリケーションサーバ 3 0 は、パーソナルコンピュータ 2 2 から受信した残高情報 B I を、セキュリティサーバ 3 1 に出力する。

セキュリティサーバ 3 1 は、アプリケーションサーバ 3 0 から入力した残高情報 B I をセッション鍵  $K_{SES}$  を用いて復号し、ログ情報 (本発明の履歴情報) を生成する。

【 0 0 5 5 】

ステップ S T 1 4 :

セキュリティサーバ 3 1 は、ステップ S T 1 3 で生成したログ情報を I C カー

ド 2 0 に書き込むためのログ書き込み情報と、ICカード 2 0 に記憶された残高情報が示す金額から請求額を減算するための減算額を示す減算情報とを含む決済処理要求 S P C（本発明の支払い処理情報）を生成し、これをセッション鍵  $K_{SE}$  を用いて暗号化する。

次に、セキュリティサーバ 3 1 は、平文の残高情報 B I と、暗号化された決済処理要求 S P C とをアプリケーションサーバ 3 0 に出力する。

アプリケーションサーバ 3 0 は、セキュリティサーバ 3 1 から入力した残高情報 B I および決済処理要求 S P C に対しての署名情報  $SIG_{APL}$  を、アプリケーションサーバ 3 0 の秘密鍵を用いて作成する。

次に、アプリケーションサーバ 3 0 は、セキュリティサーバ 3 1 から入力した残高情報 B I および決済処理要求 S P C と、署名情報  $SIG_{APL}$  とをパーソナルコンピュータ 2 2 に送信する。

#### 【 0 0 5 6 】

##### ステップ S T 1 5 :

パーソナルコンピュータ 2 2 は、アプリケーションサーバ 3 0 から受信した署名情報  $SIG_{APL}$  の正当性を、アプリケーションサーバ 3 0 の公開鍵を用いて検証し、その正当性が認められた後に以下に示す処理を行う。パーソナルコンピュータ 2 2 は、アプリケーションサーバ 3 0 から受信した残高情報 B I が示す残高、並びにステップ S T 3 でネットワークサーバ 4 0 から受信した見積もり情報が示す金額（請求額）をディスプレイに表示する。

##### ステップ S T 1 6 :

パーソナルコンピュータ 2 2 は、ステップ S T 1 5 でディスプレイに表示された残高および請求額に同意したユーザ 2 がパーソナルコンピュータ 2 2 のキーボードなどを用いて所定の指示を出すと、決済処理要求 S P C を IC カード R / W 装置 2 1 を介して IC カード 2 0 に出力する。

#### 【 0 0 5 7 】

##### ステップ S T 1 7 :

IC カード 2 0 は、パーソナルコンピュータ 2 2 から入力した決済処理要求 S P C をセッション鍵  $K_{SES}$  を用いて復号し、当該決済処理要求に応じた決済処理

を処理回路 5 1 で実行する。

具体的には、I C カード 2 0 は、処理回路 5 1 の処理によって、決済処理要求 S P C に含まれるログ書き込み情報を、I C カード 2 0 内の耐タンパ性のメモリ 5 2 に記憶する。また、I C カード 2 0 は、処理回路 5 1 の処理によって、メモリ 5 2 に記憶されている残高情報が示す残高から、決済処理要求 S P C に含まれる減算情報が示す減算額を減算し、その結果を残高情報としてメモリ 5 2 に記憶する。

#### 【 0 0 5 8 】

ステップ S T 1 8 :

I C カード 2 0 は、ステップ S T 1 7 の処理が完了すると、処理が完了したことを示す処理完了通知 P C N (本発明の支払い完了通知) を生成し、これをセッション鍵  $K_{SES}$  で暗号化した後に、パーソナルコンピュータ 2 2 およびアプリケーションサーバ 3 0 を介して、セキュリティサーバ 3 1 に送信する。

ステップ S T 1 9 :

セキュリティサーバ 3 1 は、I C カード 2 0 からの処理完了通知 P C N を受信すると、これをセッション鍵  $K_{SES}$  を用いて復号し、処理完了通知 P C N を確認した後に、決済完了通知 A C N を生成し、これをアプリケーションサーバ 3 0 を介してパーソナルコンピュータ 2 2 およびネットワークサーバ 4 0 に送信する。

ステップ S T 2 0 :

パーソナルコンピュータ 2 2 は、セキュリティサーバ 3 1 からの決済完了通知 A C N を受信すると、これに応じた情報をディスプレイに表示する。

#### 【 0 0 5 9 】

以上説明したように、ネットワークシステム 1 によれば、I C カード 2 0 のメモリ 5 2 に共通鍵  $K_C$  を記憶し、秘密鍵は記憶しない。そのため、ユーザ 2 が I C カード 2 0 を紛失した場合でも、メモリ 5 2 には秘密鍵が記憶されていないため、秘密鍵を用いてユーザ 2 の署名が不正に行われることを回避できる。

#### 【 0 0 6 0 】

また、ネットワークシステム 1 によれば、共通鍵  $K_C$  は I C カード 2 0 およびセキュリティサーバ 3 1 の内部でのみ使用されることから、共通鍵  $K_C$  が盗まれ

る危険性を低くでき、安全な取り引きを実現できると共に、鍵管理を容易にすることができる。

【0061】

また、ネットワークシステム1によれば、ICカード20に入出力される情報および要求をパーソナルコンピュータ22を介して行い、パーソナルコンピュータ22と、アプリケーションサーバ30およびネットワークサーバ40との間で情報および要求を送受信する際に、秘密鍵および公開鍵を用いた署名検証を行うことから、当該情報および要求がネットワーク5上で不正に改竄されることを回避でき、ネットワーク5を用いた取り引きの安全性を確保できる。

【0062】

また、ネットワークシステム1によれば、店舗4のネットワークサーバ40において、請求額情報BILLに対して自らの秘密鍵 $K_{SHOP,S}$ を用いて作成した署名情報SIGを付し、決済機関3のアプリケーションサーバ30において、秘密鍵 $K_{SHOP,S}$ に対応する公開鍵 $K_{SHOP,P}$ を用いて署名情報SIGを検証し、当該署名情報SIGが店舗4のネットワークサーバ40において付された正当なものであると判断することから、ユーザ2のパーソナルコンピュータ22などにおいて、不正に改竄された請求額情報BILLに基づいて決済が行われてしまうことを防止できる。

【0063】

また、ネットワークシステム1では、前述したように、パーソナルコンピュータ22は、アプリケーションサーバ30から受信した残高情報BIが示す残高、並びにネットワークサーバ40から受信した見積もり情報が示す金額（請求額）をディスプレイに表示し、その内容にユーザ2が同意した後に、アプリケーションサーバ30から受信した決済処理要求SPCをICカードR/W装置21を介してICカード20に出力する。従って、ユーザ2は、ICカード20内で最終的に行われる決済処理の内容を事前に確認でき、不正に改竄された内容で決済処理が行われることを防止できる。

また、ネットワークシステム1によれば、決済処理に伴う手順を従来に比べて少なくでき、ネットワーク5を介した情報伝送を削減でき、ネットワーク5の利

用量の削減、並びに処理時間を短縮を図れる。

また、ネットワークシステム 1 によれば、従来の S E T 方式のように、署名情報の作成および検証を多数回行う必要がない。

【 0 0 6 4 】

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、図 1 に示すように、決済機関 3 において、アプリケーションサーバ 3 0、セキュリティサーバ 3 1 および情報管理サーバ 3 2 を別々に設けた場合を例示したが、これらのサーバの機能を一つのサーバで実現してもよい。

また、上述した実施形態では、I C カード 2 0 内の残高情報をアプリケーションサーバ 3 0 に読み出す場合を例示したが、当該残高情報をアプリケーションサーバ 3 0 に読み出さないようにしてもよい。

【 0 0 6 5 】

【発明の効果】

以上説明したように、本発明によれば、共通鍵を保持した I C カードを用いて、ネットワークを介した電子商取引を安全に行う通信システム、通信装置および通信方法を提供できる。

【図面の簡単な説明】

【図 1】

図 1 は、本発明の実施形態のネットワークシステムの全体構成図である。

【図 2】

図 2 は図 1 に示す I C カードを説明するための図である。

【図 3】

図 3 は、ユーザの I C カードと、決済機関のセキュリティサーバとの間の通信方法を説明するための図である。

【図 4】

図 4 は、ユーザのパーソナルコンピュータと、店舗のネットワークサーバとの間の通信方法を説明するための図である。

【図 5】

図 5 は、ユーザのパーソナルコンピュータと、決済機関のアプリケーションサーバとの間の通信方法を説明するための図である。

【図 6】

図 6 は、図 1 に示すネットワークシステムの動作を説明するための図である。

【図 7】

図 7 は、図 1 に示すネットワークシステムの動作を説明するための図である。

【図 8】

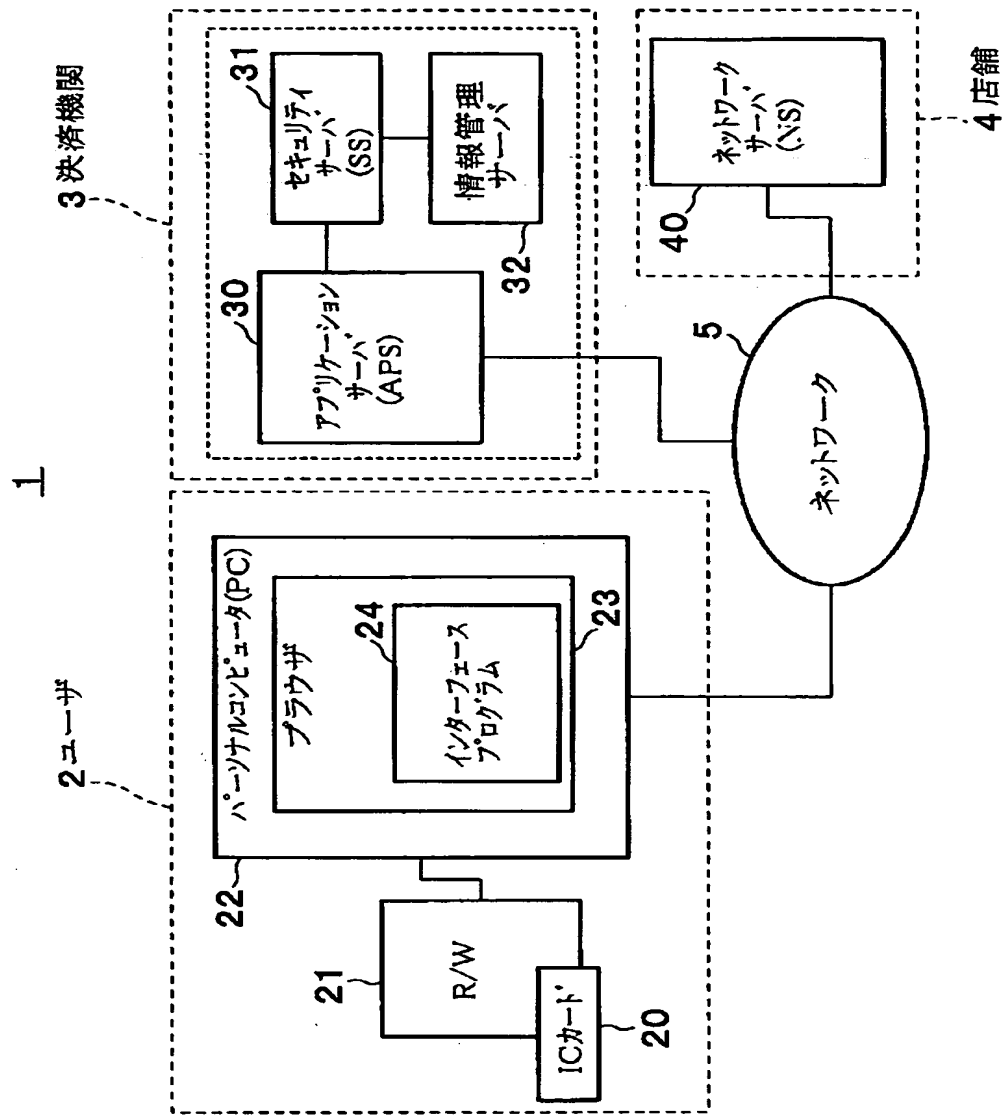
図 8 は、図 1 に示すネットワークシステムの動作を説明するための図である。

【符号の説明】

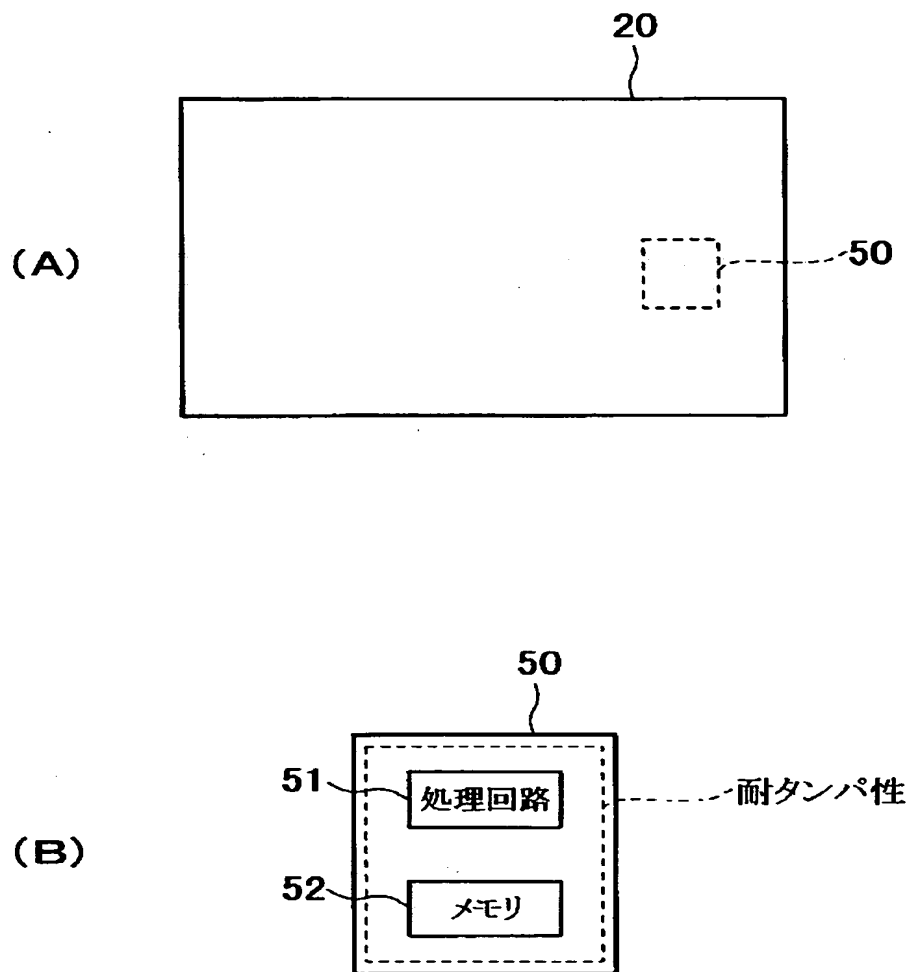
1 … ネットワークシステム、 2 … ユーザ、 3 … 決済機関、 4 … 店舗、 5 … ネットワーク、 20 … IC カード、 21 … IC カード R/W 装置、 22 … パーソナルコンピュータ、 23 … ブラウザプログラム、 24 … インターフェースプログラム、 30 … アプリケーションサーバ、 31 … セキュリティサーバ、 32 … 情報管理サーバ、 40 … ネットワークサーバ

【書類名】 図面

【図 1】

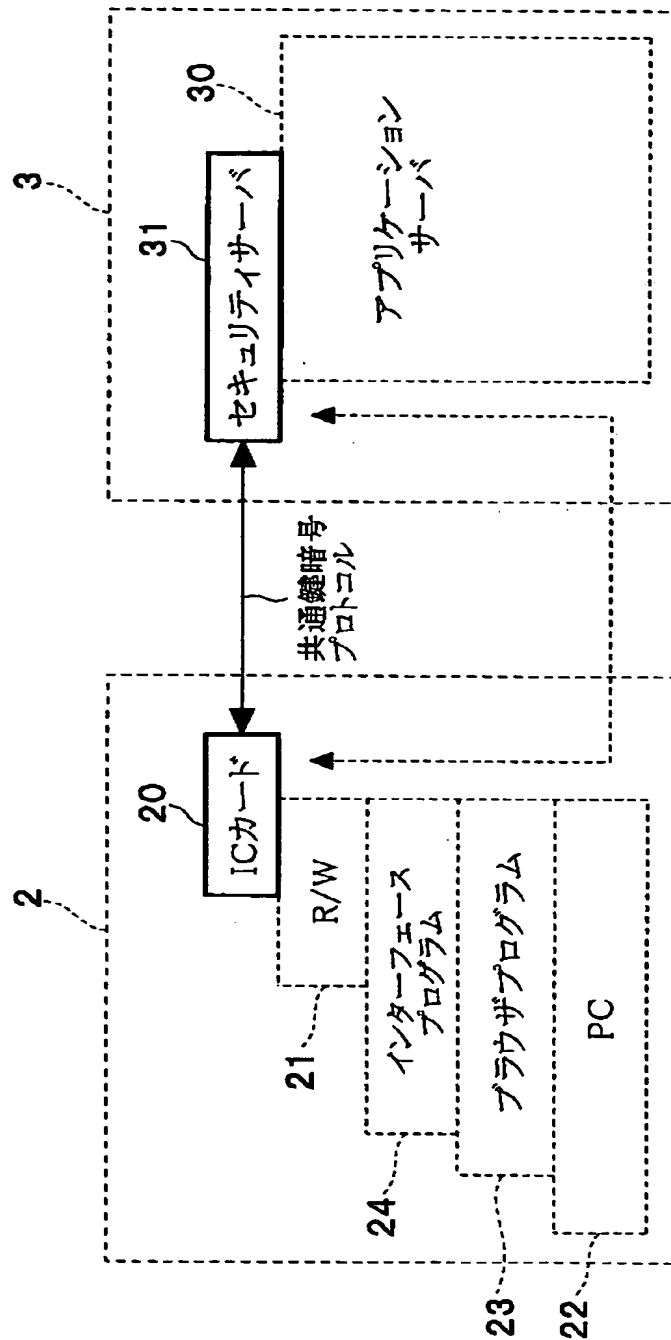


【図 2】

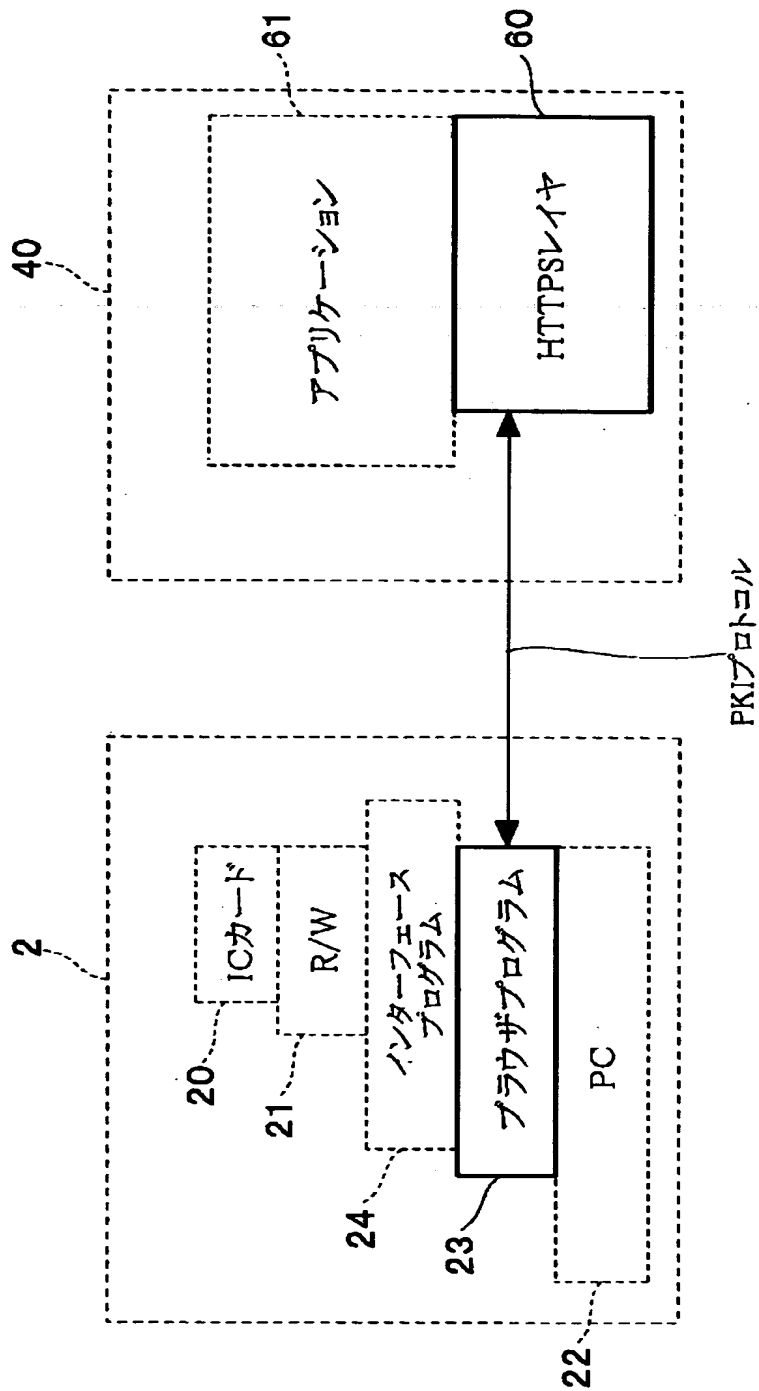




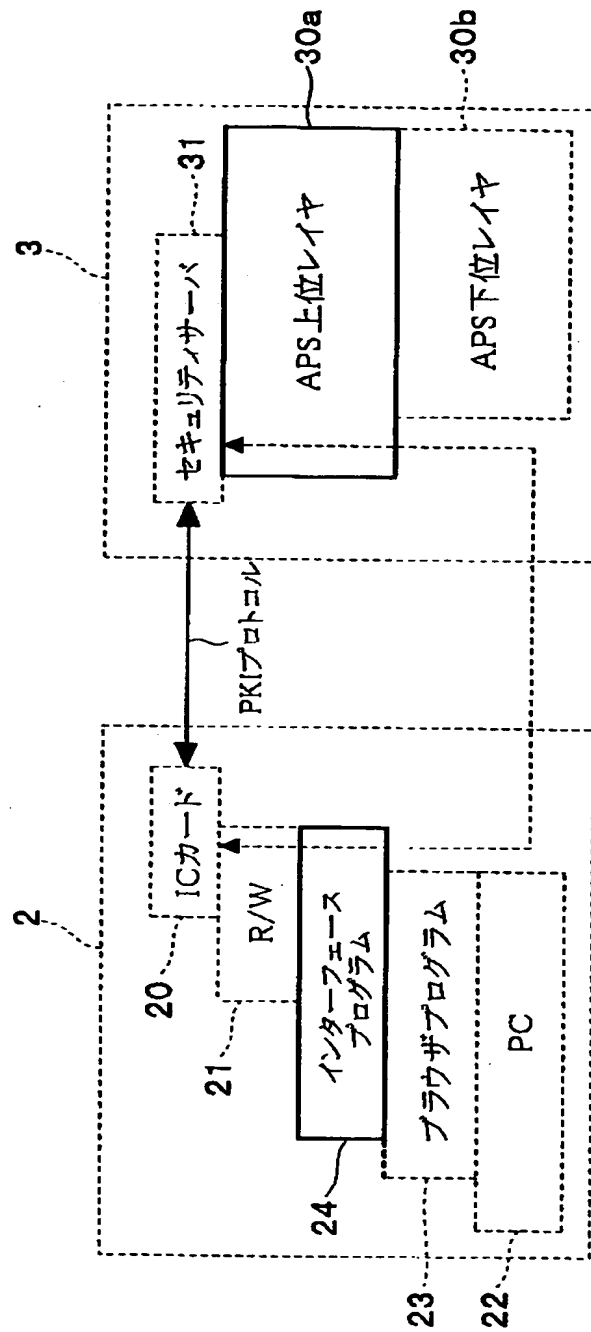
【図 3】



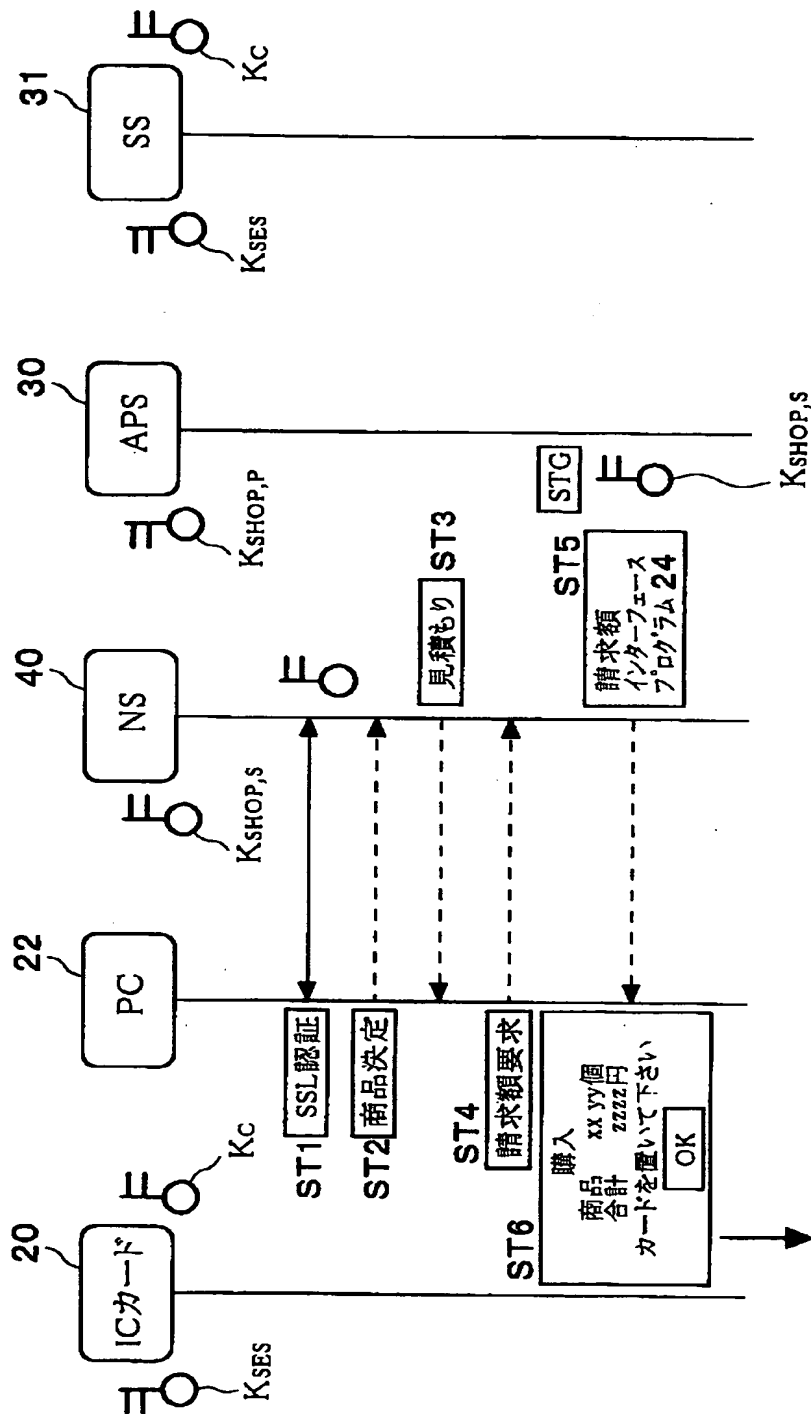
【図4】



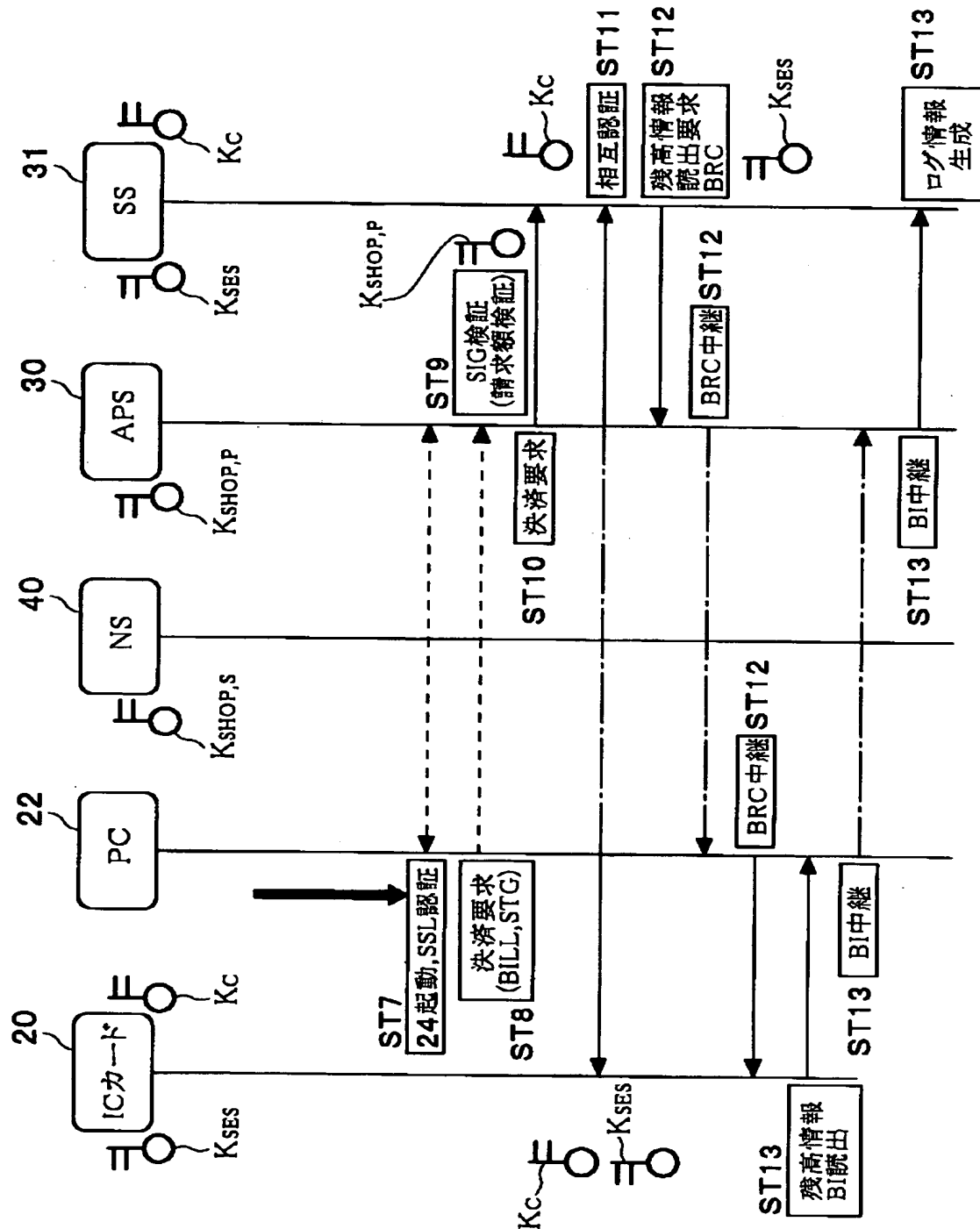
【図5】



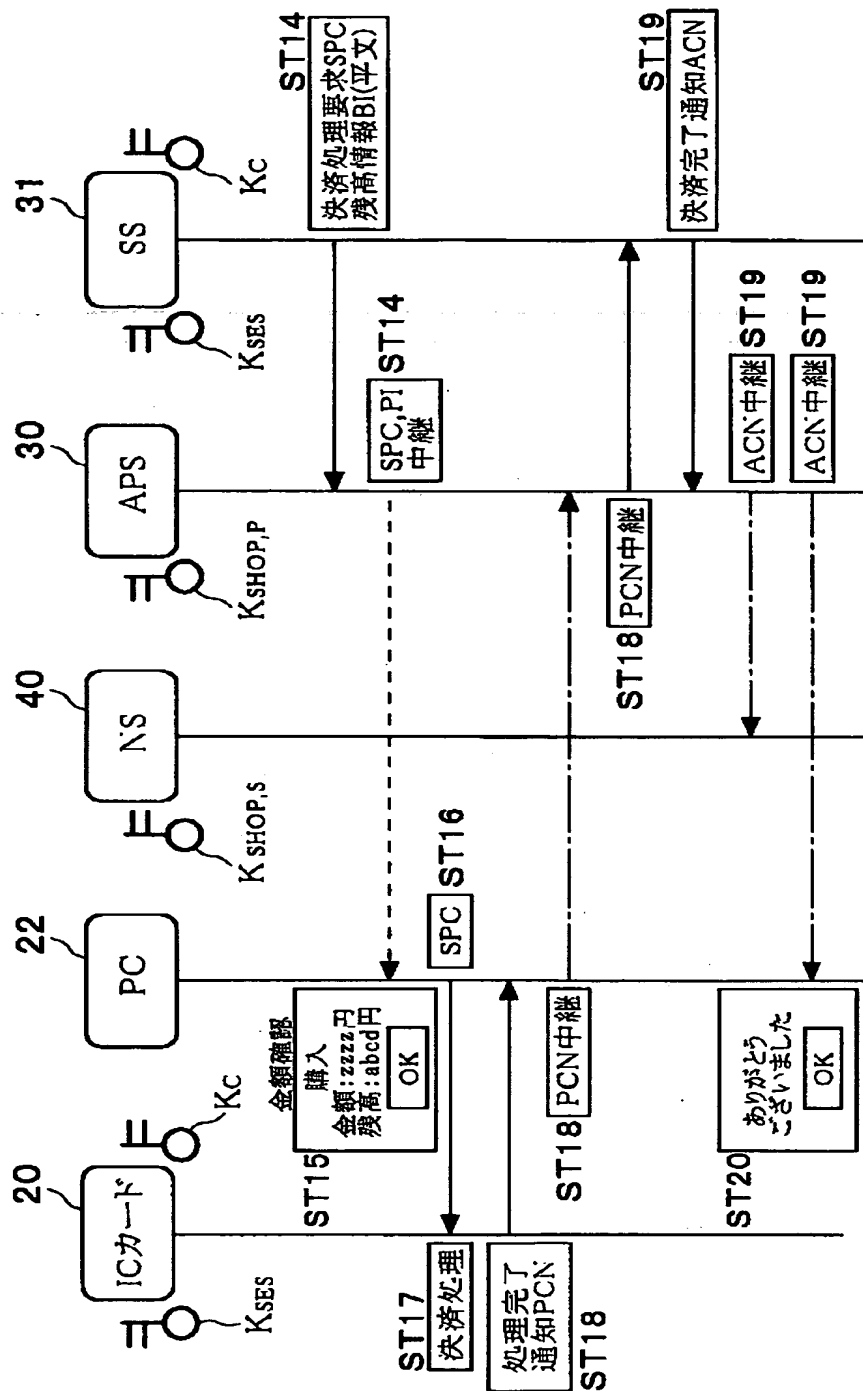
【図 6】



【図7】



【図8】



【書類名】 要約書

【要約】

【課題】 共通鍵を保持した I C カードを用いて、ネットワークを介した電子商取引を安全に行うことができる通信システムを提供する。

【解決手段】 アプリケーションサーバ 3 0 において、ネットワークサーバ 4 0 において生成された請求額情報の正当性が署名情報を用いて判断される。その後、セキュリティサーバ 3 1 において、決済処理要求が、I C カード 2 0 との間の共通鍵  $K_C$  を用いて暗号化された後に、アプリケーションサーバ 3 0 において署名情報を付してパーソナルコンピュータ 2 2 に送信される。パーソナルコンピュータ 2 2 では、署名情報を検証後に、決済処理要求を I C カード 2 0 に出力する。決済処理要求は、I C カード 2 0 において共通鍵  $K_C$  を用いて復号された後に実行される。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社